Technical Disclosure Commons

Defensive Publications Series

November 19, 2017

Access control with multiple passwords

Jie Huang

Access control with multiple passwords

ABSTRACT

Traditionally, a single user ID matched with a single password is employed for granting access to various online services and local applications. Once a user is signed in, the user can access the different services offered by the corresponding service or application. While simple, such access has potential security risks.

This disclosure provides techniques for user authentication with multiple passwords associated with a single user account. Different passwords can be associated with different access levels, e.g., read-only, read-write, and urgent. When a user logs in with a password, access to the account is granted based on the associated access level. Further, a service or application that implements multiple passwords can be set up to display certain messages (e.g., system unavailable) and to trigger an alarm upon detection of suspicious activity for the user account.

KEYWORDS

- User authentication
- Multiple passwords
- Access control
- Secure login

BACKGROUND

Traditionally, a single user ID matched with a single password is employed for granting access to various online services and local applications. Once a user is signed in, the user can access the different services offered by the corresponding service or application. While simple, such access has potential security risks.

For example, password compromise can occur e.g., if a user is forced to give out their password under duress. In another example, malicious attackers may capture user passwords, e.g., when users perform password entry while connected to an unsafe network. In another example, a user may forget to log out, e.g., after using a public computer. In these examples and other scenarios, an unauthorized user that obtains access to the user account can perform any action that is permitted for the user account.

DESCRIPTION

This disclosure describes techniques to provide multiple passwords for a single user ID. Different sets of permissions or access within an application are enabled for the different passwords for the same associated user ID. For example, a restricted access password may provide the user read-only permissions, whereas an unrestricted access password may provide read-write permissions.

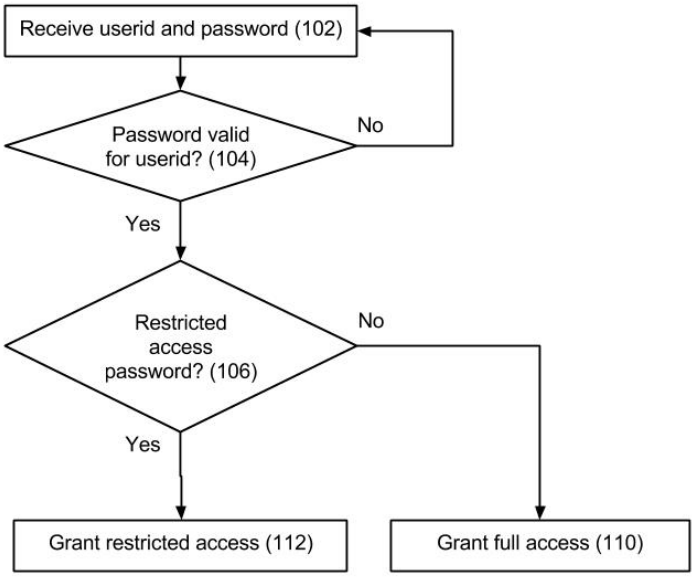

Fig. 1: Multiple passwords for one user id

Fig. 1 is an example illustration of the use of multiple passwords for user authentication using the same user ID. A user ID and a password are received (102). It is determined whether the received password is valid (104). If the password is not valid, no access is granted.

If the password is valid, it is determined whether the password received is a restricted access password (106). If the received password is a restricted access password, restricted access is a granted (112). If the received password is not a restricted password, full access is granted (110). While Fig. 1 illustrates a single restricted access password, the techniques described herein can be implemented to support multiple passwords with different levels of access.

A restricted access password is set up to grant only limited access, e.g., access to a subset of features, for the service or application. For example, a restricted access password used to log in to an online banking website may enable a user to view recent transactions and account balances, but disable money transfer. In this example, the restricted access password provides read-only permissions.

A user that wants to view a bank account, but not transact, can utilize the restricted access password for such purpose. Even if the password is compromised, an attacker's ability to cause damage is limited. For example, if the user's account is accessed by an unauthorized user using a restricted access password that attempts to engage in activities not permitted by the restricted access password, the service or application can display a warning and prevent such activities. The warning can be designed in such a way that the reason for restricted access is not revealed to the attacker, e.g., by displaying a "system unavailable" message. Further, upon detection of such suspicious activities, the service or application can lock the user account.

An unrestricted access password grants full permissions to the user. For example, when the user wants to execute banking transactions, the user can log in with a non-restricted access password, e.g., when the user is confident that the computer and network in use are secure.

Further, a password can also be set up such that use of the password triggers an alarm. For example, a password may be set up as an urgent or emergency password. When the user logs in with such a password, it triggers an alarm or notification. The service or application can take certain predefined actions, e.g., hide the user's bank account, disable access, report to authorities, etc. upon detection of such a password.

While the foregoing discussion describes multiple passwords, it is also possible to use different user IDs, in addition to different passwords, to access the same user account. For example, different user IDs can be associated with read access, read-write access, and urgent access, each with a respective password. In this case, the three user IDs are all mapped to the same user account.

CONCLUSION

This disclosure provides techniques for user authentication with multiple passwords associated with a single user account. Different passwords can be associated with different access levels, e.g., read-only, read-write, and urgent. When a user logs in with a password, access to the account is granted based on the associated access level. Further, a service or application that implements multiple passwords can be set up to display certain messages (e.g., system unavailable) and to trigger an alarm upon detection of suspicious activity for the user account.